END-TO END RECONFIGURABLE SYSTEMS: THE E^{2}R RESPONSIBILITY CHAIN CONCEPT

Didier Bourse, Karim El-Khazen, (Motorola, France)
Klaus Moessner (University of Surrey, United Kingdom)
David Grandblaise (Motorola, France)

ABSTRACT

Beside all the technological problems of SDR/CR based reconfigurable systems, there are also a number of procedural issues that have to be resolved. Reconfiguration procedures affect many, if not all actors in a communication system and assignment of responsibility for failing configurations is needed. E^{2}R [1] has undertaken research into this issue and has been developing a model capturing the areas where responsibilities will have to be assigned to ensure a coherent trail if a configuration should fail. The responsibility chain concept identifies the actors, their roles and implications and assigns the responsibilities, making the actors accountable for misbehaving configurations. Furthermore, a first approach showing the mechanisms for reconfiguration responsibility tracking on SDR terminals applying the R&TTE [2] directive is proposed.

1. INTRODUCTION

Reconfigurability, along with all the merits and advantages it offers introduces as well system design constraints on security and reliability. The fact that equipment (terminal, base station, access point, gateway) could be configured to literally any setting and could potentially implement any radio interface, be it standardised or rogue, opens the door for any type of intended or unintended faulty or even malicious system implementation. Reconfigurable equipment, in particular terminals, may easily be circulated and may appear in areas where regulation or law prohibits the reconfiguration capability or even the possession of such equipment. The problem of how to prevent the unintentional incrimination of users arises, considering the future extended roaming capabilities of the reconfigurable equipment over the different regions [3]. Furthermore, the capabilities of reconfigurable equipment will facilitate cross air interface technology roaming, and will provide the ability to adapt to any (legacy and possible future) air interface available and to download and install new software implementations in both the home but also the foreign environment.

The question of "what happens when a user wants to install software, obtained from a third party provider, on their terminal, which should operate in the network of another operator" arises. With respect to security, appropriate mechanisms are needed to verify the origin of program code prior to its integration into a reconfigurable device. Furthermore, it might be needed to supervise at runtime the functionality of specific program modules in order to ensure that downloaded code fragments do not perform unauthorized functions. Regarding reliability, appropriate techniques, mechanisms and procedures are needed to ensure that a reconfiguration action will not cause a running system to stop working correctly. This requires means for validation, fault diagnosing as well as error recovery procedures. The implications of end-to-end reconfigurability scenarios, on top of all security, reliability, stability and privacy issues, directly lead to the question of responsibility. One of the key questions to be answered will be the identification of the responsibilities for the compliance and fault-free functioning of reconfigurable equipment when reconfigured in (foreign) environments or administrative domains. This paper describes the functional and value chain in reconfigurable networks and the relations of actors involved in (re)configuration processes. It also uses examples of possible threats to associate the responsibilities of each of the actors. Finally, it provides a framework, i.e. the "E^{2}R Responsibility Chain", that offers the possibility to clearly assign the responsibilities for and during reconfiguration processes.

2. THE E^{2}R RESPONSIBILITY CHAIN CONCEPT

An End-to-End Reconfigurable communication system, focusing on the administrative roles of its actors, is depicted in Figure 1. This figure highlights the main points where reconfigurations can go wrong, it identifies the actors and defines where they would have to take responsibility for the system state.

There are a number of 'sensitive' or error prone areas (indicated by the stars in the figure) in a reconfiguration procedure and in a reconfigurable system. The stars indicate these error prone issues, **1)** highlights the problem of use of third party software. **2)** and **3)** tackle the same problem, but in these cases the software would be provided by the equipment manufacturer or operator, respectively, but the new configurations would be used in a different administrative domain (i.e. reconfiguration during roaming). **4)** tackles the issue of permitting (reconfigured) terminals to access/use an operator's Radio Network, while **5)** captures the biggest problem of responsibility in reconfigurable systems: *who can (and will) take the responsibility if a terminal is being reconfigured*. **4)** and **5)** include the prevention of spectrum misuse as well as spectrum control (e.g. in a Cognitive Radio scenario in case a user does not release the occupied spectrum).

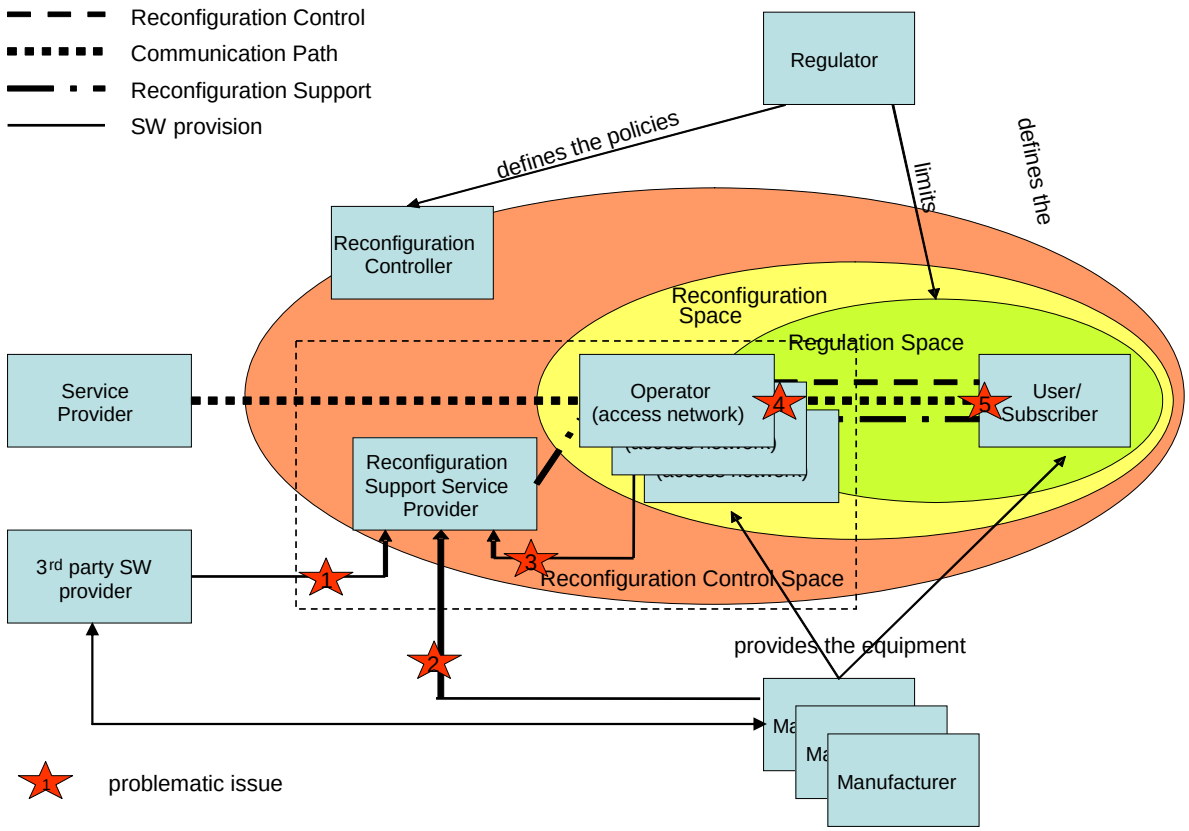

Figure 1: Actors of the Administrative Dimension and their Involvement

To be able to assign responsibilities, a clear understanding of the roles of each of the actors, in end-to-end reconfigurable environment, as well as of the relationships between them has to be established. The responsibility chain concept [4] provides definitions of the different roles, an overview on the associated responsibilities and identifies the relationships between the actors. The concept puts the responsibilities into the context of the general mobile telecoms value chain, with the aim to provide a realistic assignment of responsibilities in commercial reconfigurable radio systems. The responsibility chain defines an extended model where the actual accountability for reconfigurations is connected to the different actors within the system.

Connected to the concept of the value chain is the definition of business models for end-to-end reconfigurable systems; the responsibility chain identifies the interactions between actors encompassing information data, control data and money flow. Assumption for this is that in a reconfigurable system the roles of actors may change over time and depending on situation, hence responsibility assignment may, in various cases, be a highly dynamic process.

To cater for this dynamic-ness, E^2R proposes a scheme where the responsibility assignment is linked to a penalty scheme that is bound to the role of an actor. Figure 2 shows the general payment flow within the responsibility chain and also those parts where **penalty payments** may be applied to give incentives for standard conform configuration behavior or to recover damages created by faulty reconfigurations.

Main assumption in this model is that regulation defines for the different RATs, the policies and the limits that are to be applied in defined geographical areas and also the application timeframes. Another assumption is that equipment can not be altered without consent from an entity that acts as controller within the reconfiguration space (as depicted in Figure 1).

The penalty scheme is particularly complex, as reconfigurable terminals, as they are considered in E^2R, are free to roam through different administrative domains. The difficulties in such situations includes the tracking of the different configurations and the assignment of which actor is responsible for the tracking if the network infrastructure (and administration) is different from the 'home' network structure. If reconfigurations in foreign domains were to be 'controlled' from within the 'home' network, Reconfigurability would be limited to infrastructure based and interconnected networks. How would ad hoc or even standalone networks deal with reconfigurations?

Further, from the spectrum usage side, reconfigurable terminals would need 'local awareness' and this would

include knowledge about the radio environment as well as about the regulatory regime and spectrum access restrictions that may be in place within the area. Finally the issues of equipment circulation and possible configuration restrictions that may apply in foreign administrative domains have to be considered. This problem of downloads and reconfigurations during roaming needs particular attention.

Considering these areas and where possible problems may appear during a reconfiguration, the penalty flow mechanism of the responsibility chain will apply. The scheme foresees that any actor (again, depending on their role) who may permit a reconfiguration that results in a faulty configuration can be held liable for the damages this may cause. Figure 2 illustrates the penalty flow.

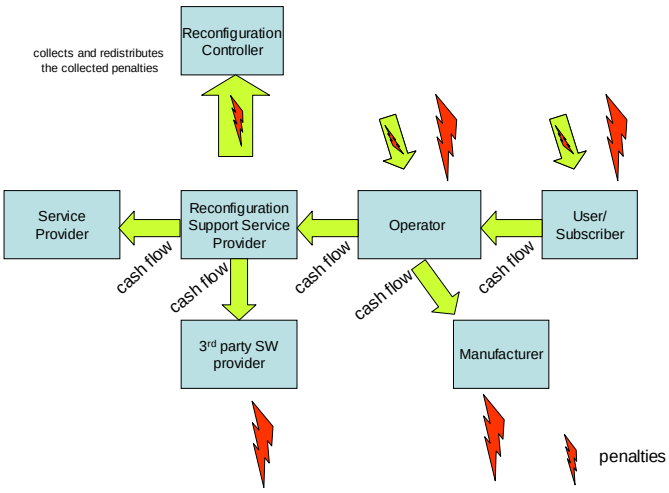

Figure 2: Revenue and Penalty Flow

As the figure indicates, 'penalty payments' will have to be made to the *Reconfiguration Controller* which supervises configurations within the current administrative domain. The Reconfiguration Controller has a mandate from the regulator to supervise the implementation of the applicable regulatory policies and to penalise misbehaving actors. The Reconfiguration Controller can also award compensation to actors that may have been negatively affected by mis-configurations.

To be able to make a sensible assignment of responsibilities, the roles of the various actors need to be clearly defined; following section will provide these definitions.

3. ACTORS AND RESPONSIBILITIES

The responsibilities may be differing depending on the market model that will be adapted for reconfigurable equipment. Each, a vertical and horizontal model are currently under discussion (in TCAM). The **vertical model** foresees that terminal reconfiguration can only be done (authorised) through the equipment manufacturer and that any software update or upgrade and any possible software configuration have to be certified and authorised by the equipment manufacturer. In the **horizontal model**, reconfigurations can be authorised by different actors and software only needs a declaration of standard compliance. The advantage of the latter is that the market for radio software would be wide open for new players. Disadvantage is that the approach is harder to control and that responsibility would be harder to assign.

As mentioned, the responsibility chain concept has been conceived with the idea of dynamically catering for the changing roles of the different actors, hence it provides the mechanisms to support both horizontal and vertical model. Looking at the responsibilities of all actors in the responsibility chain:

The **Regulator** will be responsible to define the framework for configurations and reconfigurations, for the allocation of Spectrum, definition of use and usage policies and for the definition of usage rules and penalties for violation of responsibilities.

The **Reconfiguration Controller** (i.e. a type of system monitor) must perform the monitoring of: Standard Conformity and Certification, of Security, and of the Spectrum Manager. Its responsibilities include the supervision of spectrum management and the registration of equipments configuration history. Additionally, in the *horizontal market*, it has to monitor and police the implementation of spectrum usage policies and it has to monitor and police the implementation of equipment updates.

The **Service Provider** must ensure the authenticity of the content, it must make provisions to ensure content delivery and optionally it may request updates, but has no responsibilities associated to this request.

The **Reconfiguration Support Service Provider** (RSSP) is a new entity, it has to provide control and security mechanisms to facilitate secure download, it has to verify the compliance of download software as well as the suitability of the intended configuration (HW/SW combination). In the *vertical model* is the additional requirement that the RSSP must ensure that only manufacturer endorsed software can be downloaded and installed. In the *horizontal model*, the RSSP must facilitate the run-time evaluation of configuration software and it must provide the mechanisms to prevent a terminal from reconfiguring.

The **Network Operator** has to provide the infrastructure and secure connectivity for communication, signalling and SW downloads; it is responsible for the proper operation of equipment within their administrative domain. In the

vertical model it has to prevent unauthorised parties to access the network, while in the horizontal model it has to facilitate SW updates by providing suitable connectivity.

The **Equipment Manufacturer** is responsible for the proper operation of their hardware in terms of radio performance (e.g. linearity of power amplifier, …), and it is responsible for the proper operation of the support SW provided with the HW, in terms of primitives (e.g. basic security, …). Additional requirements for the *vertical model* include that it has to prevent users from downloading unauthorised SW, to prevent the HW from using/accepting unauthorised SW, to ensure suitability of the initially provided radio SW and ensure suitability of downloadable radio SW. Additional requirements for the *horizontal model* are to ensure suitability of the initially provided radio SW (if any), to ensure suitability of any other downloadable radio SW he may provide, to provide descriptions of potential problems, limitations and system APIs and to facilitate certification of configuration software for their radio hardware.

The **Software Provider** has to implement/provide an established authentication mechanism (preventing impersonation), and to implement security features when providing SW (e.g. security of radio SW download). For the vertical model, they have to provide radio SW in accordance to agreements with manufacturer of the HW. Additional horizontal requirements are to declare with which HWs a SW may be used of for which HWs a SW has been designed and also to make a declaration of conformity in accordance with the statement of intended (modified) use.

Finally the **User/Subscriber** has to read instructions and act according to them, and in particular, they have to be aware of local possibilities/restrictions (in terms of usability of radio interfaces, maximum power levels, etc.). In the *vertical model*, the user is expected to obtain configuration SW from the appropriate manufacturer (exclusively!), while in the *horizontal model* they are expected to obtain configuration SW exclusively from authorised sources (in accordance with the HW used).

4. SHAPING A FRAMEWORK FOR END-TO-END RECONFIGURABLE SYSTEMS

The E^2R project aims to develop a regulatory scheme where reconfigurable equipment can be used to ensure a robust end-to-end connectivity (secure, reliable and stable operation).. For this purpose, E^2R has started to collate opinions and information from regulator organizations world wide. The E^2R consortium started to collect and analyse the trends of the global regulatory community. The approach followed was based on development, distribution and analysis of a regulatory questionnaire. The outcomes of this consultation have flown into the definition of a regulatory framework that covers the main areas related to SDR/CR and reconfigurable technologies.

The questionnaire covered a number of areas and issues that will influence the use and distribution of reconfigurable equipment in the commercial domain. The issues include spectrum management, terminal reconfigurability, network reconfigurability, and the general question of responsibility. Following the responsibility chain concept [4], a number of issues were of particular interest for (regulatory) rule makers, and the relevant questions were asked in the questionnaire:

- SDR technology will allow new actors to enter the market, also, the role of some of the incumbent actors will change even during operation of a reconfigurable terminal, the question of which actor takes the responsibility for third party software and who vouches that such software can be used to implement a radio protocol on the platform built by a specific manufacturer.
- Reconfiguration Software may be provided by the equipment manufacturer or operator, respectively, and the configurations would be used in a different administrative domain.
- The matter about whether or not to permit (reconfigured) terminals to access/use an operator's Radio Access Technology (RAT).
- Finally, the question about who can (and will) take the responsibility if a terminal is being reconfigured.

The latter two questions dealt with the need to prevent the misuse of spectrum (e.g. in the Cognitive Radio approach, when a user does not release the spectrum) as well as the spectrum control.

The framework covers both spectrum as well as equipment related issues of regulation. As a first outcome, a scheme for certification of reconfigurable equipment was developed. This is described in section 5.

5. CERTIFICATION OF EQUIPMENT – THE R&TTE DIRECTIVE AND RECONFIGURABILITY

Taking the R&TTE directive for equipment certification as example, the mechanisms defined there provide already some room for flexibility (see [2] for details). The R&TTE directive allows the manufacturer to self certify equipment they produce. For this a manufacturer has to design and specify their equipment according to a set of **harmonised standards**, the equipment has to fulfil the **Essential Requirements** captured in the standard and the manufacturer has to make a **declaration of intended use**. Further they have to provide a **declaration of conformity** (i.e. conforming to the harmonised standards), to apply the

CE marking and to add the required **documentation** (Article 6.3) of how the equipment ought to be used.

This process is shown in the figure below (figure 3).

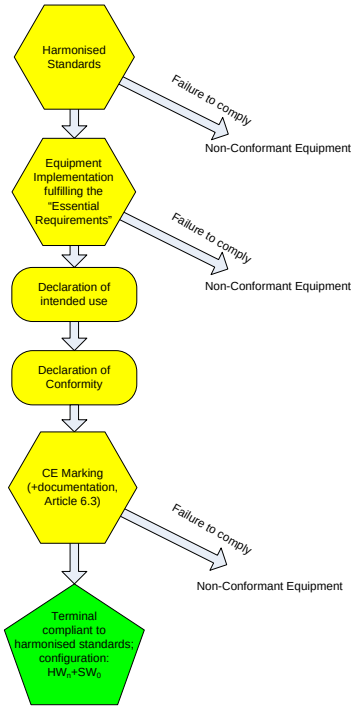

Figure 3 R&TTE Equipment Certification

Based on this procedure, reconfigurable equipment may be certified even after initial delivery through the manufacturer. Taking (certified) equipment (with reconfiguration capability), see figure 4, any new, or intended configuration will again have to comply to the set of **harmonised standards**. The combination of a reconfigurable terminal and the new (or incremental) software installation have to fulfil the **essential requirements** and a **declaration of the intended use** (of the new HW/SW combination) has to be made. With the **declaration of conformity**, the actor who undertakes the reconfiguration will have **to take the responsibility for the configuration**. Then a new **CE mark** and the required **documentation** have to be provided (i.e. both could be implemented in SW and be accessible via the telephone screen).

6. CONCLUSIONS

This paper deals with the assignment of responsibilities for any unwanted effects that Reconfigurability may and can cause. We have developed a scheme (the responsibility chain) where responsibility for reconfiguration can be assigned to the different actors involved. As Reconfigurability can lead to a change in roles of the actors, the scheme has to provide sufficient flexibility to assign responsibility to different partners, depending on the reconfiguration situation. The paper describes this complexity, as well as the roles of the actors and finally provides an example of how the responsibility for reconfigurable equipment can be assigned while using and maintaining the existing regulatory mechanisms (i.e. the R&TTE directive).

Figure 4 Extended R&TTE Equipment Certification for Reconfigurable Equipment

7. ACKNOWLEDGMENTS

This work has been performed in the framework of the EU funded project E²R. The authors would like to acknowledge in particular MM. Paul Bender and Georges de Brito, but also the contributions of their other colleagues from the E²R consortium.

8. REFERENCES

[1] End-to-End Reconfigurability (E²R), FP6 IST-2003-507995, http://www.e2r.motlabs.com

[2] R&TTE Directive, http://europa.eu.int/comm/enterprise/rtte/

[3] W. Tuttlebee, *Software Defined Radio: Origins, Drivers and International Perspectives*, Wiley, March 2002.

[4] K. Moessner, D. Bourse, K. El-Khazen, D. Grandblaise, *The Responsibility Chain in End-to End Reconfigurable Systems*, E^2R Workshop on End-to-End Reconfigurability, Barcelona, Spain, 05.09.2004